Please note that US-CERT has changed the look and scope of the Cyber Security Bulletin.

The US-CERT Cyber Security Bulletin provides a summary of new vulnerabilities that have been recorded by the National Institute of Standards and Technology (NIST) National Vulnerability Database (NVD) in the past week. The NVD is sponsored by the Department of Homeland Security (DHS) National Cyber Security Division (NCSD) / United States Computer Emergency Readiness Team (US-CERT). For modified or updated entries, please visit the NVD, which contains historical vulnerability information.

The vulnerabilities are based on the CVE vulnerability naming standard and are organized according to severity, determined by the Common Vulnerability Scoring System (CVSS) standard. The division of high, medium, and low severities correspond to the following scores:

- **High** - Vulnerabilities will be labeled High severity if they have a CVSS base score of 7.0 - 10.0
- **Medium** - Vulnerabilities will be labeled Medium severity if they have a CVSS base score of 4.0 - 6.9
- **Low** - Vulnerabilities will be labeled Low severity if they have a CVSS base score of 0.0 - 3.9

Entries may include additional information provided by organizations and efforts sponsored by US-CERT. This information may include identifying information, values, definitions, and related links. Patch information is provided when available. Please note that some of the information in the bulletins is compiled from external, open source reports and is not a direct result of US-CERT analysis.

High Vulnerabilities

Primary Vendor -- Product	Description	Discovered Published	CVSS Score	Source & Patch Info
4Images -- Image Gallery Management System	Multiple SQL injection vulnerabilities in 4images 1.7.1 and earlier allow remote attackers to execute arbitrary SQL commands via the sessionid parameter in (1) top.php and (2) member.php. NOTE: this issue has also been reported to affect 1.7.2.	2006-04-28 2006-05-05	7.0	CVE-2006-2214 BUGTRAQ BID FRSIRT SECUNIA XF
AZNEWS -- AZNEWS	SQL injection vulnerability in news.php in AZNEWS allows remote attackers to execute arbitrary SQL commands via the ID parameter.	unknown 2006-05-02	7.0	CVE-2006-2136 EVULN FRSIRT SECUNIA
BoonEx -- Barracuda	SQL injection vulnerability in index.php in BoonEx Barracuda 1.1 and earlier allows remote attackers to execute arbitrary SQL commands via the (1) link_dir_target and (2) link_id_target parameter, possibly involving the link_edit functionality.	unknown 2006-05-01	7.0	CVE-2006-2133 BLOGSPOT
CGIIRC -- CGIIRC	Multiple buffer overflows in client.c in CGI:IRC (CGIIRC) before 0.5.8 might allow remote attackers to execute arbitrary code via (1) cookies or (2) the query string.	2006-04-30 2006-05-02	7.0	CVE-2006-2148 OTHER-REF OTHER-REF OTHER-REF OTHER-REF FRSIRT SECUNIA
EMC Corporation -- Retrospect	EMC Retrospect for Windows 6.5 before 6.5.382, 7.0 before 7.0.344, and 7.5 before 7.5.1.105 does not drop privileges before opening files, which allows local users to execute arbitrary code via the File>Open dialog.	unknown 2006-05-03	7.0	CVE-2006-2154 FRSIRT SECUNIA
FileProtection Express -- FileProtection Express	FileProtection Express 1.0.1 and earlier allows remote attackers to bypass authentication via a cookie with an Admin value of 1.	unknown 2006-05-04	10.0	CVE-2006-2168 BUGTRAQ BID
Gene6 -- G6 FTP Server	Buffer overflow in Gene6 FTP Server 3.1.0 allows remote authenticated attackers to cause a denial of service (crash) and possibly execute arbitrary code via a long argument to (1) MKD or (2) XMKD, as demonstrated by the Infigo FTPStress Fuzzer.	2005-11-12 2006-05-04	7.0	CVE-2006-2172 BUGTRAQ OTHER-REF BID
JMK Web Scripts -- JMK Picture Gallery	JMK's Picture Gallery allows remote attackers to bypass authentication via a direct request to admin_gallery.php3, possibly related to the add action.	2006-05-01 2006-05-01	7.0	CVE-2006-2118 BUGTRAQ BID
JSBoard -- JSBoard	Cross-site scripting (XSS) vulnerability in the parse_query_str function in include/print.php in JSBoard 2.0.10 and 2.0.11, and possibly other versions before 2.0.12, allows remote attackers to inject arbitrary web script or HTML via parameters that are set as global variables within the program, as demonstrated using the table parameter to login.php.	unknown 2006-05-02	7.0	CVE-2006-2109 KLINK
Microsoft -- Internet Explorer	Unspecified vulnerability in Internet Explorer 6.0 on Microsoft Windows XP SP2 allows remote attackers to execute arbitrary code, a variant of CVE-2006-1992.	unknown 2006-05-05	7.0	CVE-2006-2218 BID SECUNIA

OpenPHPNuke -- OpenPHPNuke	PHP remote file inclusion vulnerability in master.php in OpenPHPNuke and 2.3.3 earlier allows remote attackers to execute arbitrary PHP code via a URL in the root_path parameter.	2006-04-29 2006-05-02	7.0	CVE-2006-2137 Milw0rm OPEN PHP NUKE FRSIRT SECUNIA
Pentasoft Corp. -- Avactis Shopping Cart	Multiple SQL injection vulnerabilities in Avactis Shopping Cart 0.1.2 and earlier allow remote attackers to execute arbitrary SQL commands via the (1) category_id parameter in (a) store_special_offers.php and (b) store.php, and (2) prod_id parameter in (c) cart.php and (d) product_info.php. NOTE: this issue also produces resultant full path disclosure from invalid SQL queries.	unknown 2006-05-04	7.0	CVE-2006-2164 OTHER-REF
phpBB Group -- phpBB TopList	PHP remote file inclusion vulnerability in toplist.php in phpBB TopList 1.3.8 and earlier, when register_globals is enabled, allows remote attackers to include arbitrary files via the phpbb_root_path parameter.	unknown 2006-05-03	7.0	CVE-2006-2151 OTHER-REF FRSIRT SECUNIA
phpBB Group -- phpBB Advanced Guestbook	PHP remote file inclusion vulnerability in admin/addentry.php in phpBB Advanced Guestbook 2.4.0 and earlier, when register_globals is enabled, allows remote attackers to include arbitrary files via the phpbb_root_path parameter.	unknown 2006-05-03	7.0	CVE-2006-2152 OTHER-REF FRSIRT SECUNIA
PlaNet Concept -- planetGallery	planetGallery allows remote attackers to gain administrator privileges via a direct request to admin/gallery_admin.php.	2006-05-01 2006-05-01	7.0	CVE-2006-2116 BUGTRAQ BID
Ruperts News -- Ruperts News	SQL injection vulnerability in login.php in Ruperts News allows remote attackers to execute arbitrary SQL commands via the username parameter.	unknown 2006-05-02	7.0	CVE-2006-2135 EVULN FRSIRT SECUNIA
Servous -- sBLOG	SQL injection vulnerability in search.php in Servous sBLOG 0.7.2 allows remote attackers to execute arbitrary SQL commands via the keyword parameter. NOTE: this issue can be used to trigger path disclosure. In addition, it might be primary to vector 1 in CVE-2006-1135.	2006-05-02 2006-05-04	10.0	CVE-2006-2189 BUGTRAQ SUBJECTZERO BID
SmartWin Technology -- CyberOffice Warehouse Builder	Multiple SQL injection vulnerabilities in CyberBuild allow remote attackers to execute arbitrary SQL commands via the (1) SessionID parameter to login.asp or (2) ProductIndex parameter to browse0.htm.	2006-05-01 2006-05-04	7.0	CVE-2006-2179 OTHER-REF FRSIRT SECUNIA
TrueCrypt Foundation -- TrueCrypt	Untrusted search path vulnerability in Truecrypt 4.1, when running suid root on Linux, allows local users to execute arbitrary commands and gain privileges via a modified PATH environment variable that references a malicious mount command.	2005-12-14 2006-05-04	7.0	CVE-2006-2183 MLIST OTHER-REF FRSIRT OSVDB SECUNIA
Ultr@VNC -- Ultr@VNC	The MS-Logon authentication scheme in UltraVNC (aka Ultr@VNC) 1.0.1 uses weak encryption (XOR) for challenge/response, which allows remote attackers to gain privileges by sniffing and decrypting passwords.	2006-05-03 2006-05-05	10.0	CVE-2006-2206 BUGTRAQ BID
Zenphoto -- Zenphoto	Multiple cross-site scripting (XSS) vulnerabilities in zenphoto 1.0.1 beta and earlier allow remote attackers to inject arbitrary web script or HTML via the (1) a parameter in i.php, and the (2) album and (3) image parameters in index.php.	2006-04-02 2006-05-04	7.0	CVE-2006-2187 BUGTRAQ ZONE14 BID

Back to top

Medium Vulnerabilities

Primary Vendor -- Product	Description	Discovered Published	CVSS Score	Source & Patch Info
321soft -- PhP-Gallery	Cross-site scripting (XSS) vulnerability in index.php in 321soft PhP-Gallery 0.9 allows remote attackers to inject arbitrary web script or HTML via the path parameter. NOTE: this issue might be resultant from the directory traversal vulnerability.	2006-05-03 2006-05-05	4.7	CVE-2006-2210 OTHER-REF BID FRSIRT SECUNIA
Advanced Poll -- Advanced Poll	SQL injection vulnerability in include/class_poll.php in Advanced Poll 2.0.4 allows remote attackers to execute arbitrary SQL commands via the User-Agent HTTP header.	unknown 2006-05-01	5.6	CVE-2006-2130 EVULN
Albinator -- Albinator	Multiple PHP remote file inclusion vulnerabilities in (1) eday.php, (2) eshow.php, or (3) forgot.php in albinator 2.0.8 and earlier allow remote attackers to execute arbitrary PHP code via a URL in the Config_rootdir parameter.	2006-05-03 2006-05-04	4.7	CVE-2006-2182 OTHER-REF BID FRSIRT

Albinator -- Albinator	Multiple cross-site scripting (XSS) vulnerabilities in Albinator 2.x allow remote attackers to inject arbitrary web script or HTML via the (1) cid parameter to dlisting.php or (2) preloadSlideShow parameter to showpic.php. NOTE: the provenance of this information is unknown; the details are obtained solely from third party information.	2006-05-04 2006-05-05	4.7	CVE-2006-2215 SECUNIA
ArGoSoft -- ArGoSoft FTP Server	Buffer overflow in ArgoSoft FTP Server allows remote attackers to execute arbitrary code via Unicode in the RNTO command, as demonstrated by the Infigo FTPStress Fuzzer.	2005-11-12 2006-05-04	4.7	CVE-2006-2170 BUGTRAQ OTHER-REF BID FRSIRT SECUNIA
Avalon Ltd -- MaxTrade	SQL injection vulnerability in pocategories.php in MaxTrade 1.0.1 and earlier allows remote attackers to execute arbitrary SQL commands via the (1) categori and (2) stranica parameters.	2006-04-30 2006-05-01	4.7	CVE-2006-2126 OTHER-REF FRSIRT SECUNIA
Avatic -- Aardvark Topsites PHP	PHP remote file inclusion vulnerability in sources/lostpw.php in Aardvark Topsites PHP 4.2.2 and earlier, when register_globals is enabled, allows remote attackers to execute arbitrary PHP code via the CONFIG[path] parameter, as demonstrated by including a GIF that contains PHP code.	2006-05-01 2006-05-03	4.7	CVE-2006-2149 OTHER-REF FRSIRT SECUNIA
Blog Mod -- Blog Mod	SQL injection vulnerability in weblog_posting.php in Blog Mod 0.2.x allows remote attackers to execute arbitrary SQL commands via the r parameter.	2006-04-29 2006-05-01	4.7	CVE-2006-2127 BUGTRAQ BID
Cisco -- Cisco Unity Express	Unspecified vulnerability in the HTTP management interface in Cisco Unity Express (CUE) 2.2(2) and earlier, when running on any CUE Advanced Integration Module (AIM) or Network Module (NM), allows remote authenticated attackers to reset the password for any user with an expired password.	unknown 2006-05-04	6.0	CVE-2006-2166 CISCO BID FRSIRT SECTRACK SECUNIA
CoolMenus -- CoolMenus	PHP remote file inclusion vulnerability in index.php in CoolMenus allows remote attackers to execute arbitrary code via a URL in the page parameter. NOTE: the original report for this issue is probably erroneous, since CoolMenus does not appear to be written in PHP.	2006-04-28 2006-05-01	4.9	CVE-2006-2122 BUGTRAQ OTHER-REF OTHER-REF BID
DeltaScripts -- Pro Publish	Multiple SQL injection vulnerabilities in Pro Publish 2.0 allow remote attackers to execute arbitrary SQL commands via the (1) email parameter to login.php, (2) password parameter to login.php, (3) find_str parameter to search.php, or (4) artid parameter to art.php.	2006-04-30 2006-05-01	4.7	CVE-2006-2128 OTHER-REF BID FRSIRT SECUNIA
DMCounter -- DMCounter	PHP remote file inclusion vulnerability in kopf.php in DMCounter 0.9.2-b allows remote attackers to execute arbitrary PHP code via a URL in the rootdir parameter.	2006-05-01 2006-05-02	4.7	CVE-2006-2144 BUGTRAQ BID
EMC Corporation -- Retrospect	EMC Retrospect for Windows 6.5 before 6.5.382, 7.0 before 7.0.344, and 7.5 before 7.5.1.105 allows local users to execute arbitrary code by replacing the Retrospect.exe file, possibly due to improper file permissions.	unknown 2006-05-03	4.9	CVE-2006-2155 OTHER-REF FRSIRT SECUNIA
FileZilla -- FileZilla Server	Buffer overflow in FileZilla FTP Server allows remote authenticated attackers to cause a denial of service and possibly execute arbitrary code via (1) the MLSD command or (2) the remote server interface, as demonstrated by the Infigo FTPStress Fuzzer.	2005-11-12 2006-05-04	4.7	CVE-2006-2173 BUGTRAQ OTHER-REF BID
FtrainSoft -- Fast Click	PHP remote file inclusion vulnerability in FtrainSoft Fast Click 2.3.8 and earlier allows remote attackers to execute arbitrary PHP code via a URL in the path parameter to (1) show.php or (2) top.php.	2006-05-03 2006-05-04	4.7	CVE-2006-2175 OTHER-REF OTHER-REF FRSIRT SECUNIA
Harold Bakker -- HB-NS	Multiple SQL injection vulnerabilities in index.php in HB-NS 1.1.6 allow remote attackers to execute arbitrary SQL commands via the (1) topic or (2) id parameter.	2006-04-29 2006-05-02	4.7	CVE-2006-2145 OTHER-REF BID SECUNIA
Harold Bakker -- HB-NS	Multiple cross-site scripting (XSS) vulnerabilities in index.php in HB-NS 1.1.6 allow remote attackers to inject arbitrary web script or HTML via the (1) poster_name, (2) poster_email, (3) poster_homepage, or (4) message parameter.	2006-04-29 2006-05-02	4.7	CVE-2006-2146 OTHER-REF BID SECUNIA
Invision Power Services -- Invision Gallery	SQL injection vulnerability in post.php in Invision Gallery 2.0.6 allows remote attackers to execute arbitrary SQL commands via the album parameter.	2006-05-02 2006-05-04	4.7	CVE-2006-2202 BUGTRAQ BID FRSIRT SECTRACK SECUNIA

				BUGTRAQ OSVDB
Invision Power Services -- Invision Power Board	SQL injection vulnerability in index.php in Invision Power Board allows remote attackers to execute arbitrary SQL commands via the pid parameter in a reputation action. NOTE: the provenance of this information is unknown; the details are obtained solely from third party information.	2006-05-04 2006-05-05	4.7	CVE-2006-2217 BID
Jgaa -- WarFTPd	Buffer overflow in WDM.exe in WarFTPD allows remote attackers to execute arbitrary code via unspecified arguments, as demonstrated by the Infigo FTPStress Fuzzer.	2005-11-12 2006-05-04	4.7	CVE-2006-2171 BUGTRAQ OTHER-REF BID
KarjaSoft -- Sami FTP Server	Buffer overflow in KarjaSoft Sami FTP Server 2.0.2 and earlier allows remote attackers to execute arbitrary code via unspecified username and password input while connecting to the server.	2006-05-04 2006-05-05	4.7	CVE-2006-2212 BUGTRAQ BID
Kerio -- MailServer	Unspecified vulnerability in Kerio MailServer before 6.1.4 has unknown impact and remote attack vectors related to a "possible bypass of attachment filter."	2006-05-02 2006-05-05	4.7	CVE-2006-2203 OTHER-REF FRSIRT SECUNIA
Limbo CMS -- Limbo CMS	PHP remote file inclusion vulnerability in classes/adodbt/sql.php in Limbo CMS 1.04 and earlier allows remote attackers to execute arbitrary PHP code via a URL in the classes_dir parameter.	2006-05-01 2006-05-02	4.7	CVE-2006-2142 OTHER-REF FRSIRT SECUNIA
Network Administration Visualized -- Network Administration Visualized	Multiple SQL injection vulnerabilities in the report interface in Network Administration Visualized (NAV) before 3.0.1 allow remote attackers to execute arbitrary SQL commands via unknown vectors.	2006-04-28 2006-05-01	4.7	CVE-2006-2123 OTHER-REF BID OSVDB FRSIRT SECUNIA
Océ North America -- 3122 Printer Océ North America -- 3121 Printer	parser.exe in Océ (OCE) 3121/3122 Printer allows remote attackers to cause a denial of service (crash or reboot) via a long request, possibly triggering a buffer overflow.	2006-03-29 2006-04-29	5.0	CVE-2006-2108 OTHER-REF BID SECUNIA
Orbitscripts -- OrbitHYIP	Multiple cross-site scripting (XSS) vulnerabilities in OrbitHYIP 2.0 and earlier allow remote attackers to inject arbitrary web script via the (1) referral parameter to signup.php or (2) id parameter to members.php.	2006-04-30 2006-05-02	4.7	CVE-2006-2140 OTHER-REF FRSIRT SECUNIA
PHP Arena -- paCheckBook	Multiple SQL injection vulnerabilities in index.php in PHP Arena paCheckBook 1.1 allow remote attackers to execute arbitrary SQL commands via (1) the transtype parameter in an add action or (2) entry parameter in an edit action. NOTE: the provenance of this information is unknown; the details are obtained from third party information.	2006-05-03 2006-05-05	4.7	CVE-2006-2209 BID OTHER-REF
PHP Design X -- PHP Linkliste	Multiple cross-site scripting (XSS) vulnerabilities in links.php in PHP Linkliste 1.0b allow remote attackers to inject arbitrary web script or HTML via the (1) new_input, (2) new_url, or (3) new_name parameter.	2006-05-02 2006-05-04	4.7	CVE-2006-2176 OTHER-REF FRSIRT SECUNIA
phpBB Group -- phpBB	PHP remote file inclusion vulnerability in /includes/kb_constants.php in Knowledge Base Mod for PHPbb 2.0.2 and earlier allows remote attackers to execute arbitrary PHP code via a URL in the module_root_path parameter.	2006-04-29 2006-05-02	5.6	CVE-2006-2134 Milw0rm FRSIRT SECUNIA
phpBB Group -- phpBB TopList	PHP remote file inclusion vulnerability in top/list.php in phpBB TopList 1.3.8 and earlier allows remote attackers to include arbitrary files via the returnpath parameter.	2006-04-28 2006-05-03	4.7	CVE-2006-2150 BUGTRAQ
SmartWin Technology -- CyberOffice Warehouse Builder	Mulitiple cross-site scripting (XSS) vulnerabilities in CyberBuild allow remote attackers to inject arbitrary web script or HTML via the (1) SessionID parameter to login.asp, (2) ProductIndex parameter to browse0.htm, (3) rowcolor parameter to result.asp, or (4) heading parameter to result.asp. NOTE: vectors 1 and 2 might be resultant from SQL injection.	2006-05-01 2006-05-04	4.7	CVE-2006-2178 OTHER-REF FRSIRT SECUNIA
Stadtaus -- Guestbook Script	Dynamic variable evaluation vulnerability in index.php in Stadtaus Guestbook Script 1.7 and earlier, when register_globals is enabled, allows remote attackers to modify arbitrary program variables via parameters, which are evaluated as PHP variable variables, as demonstrated by performing PHP remote file inclusion using the include_files array parameter.	unknown 2006-05-03	4.7	CVE-2006-2158 OTHER-REF OTHER-REF
Turnkey Solutions -- SunShop Shopping Cart	Multiple cross-site scripting (XSS) vulnerabilities in SunShop 3.5 and earlier allow remote attackers to inject arbitrary web script or HTML via the (1) prevaction, (2) previd, (3) prevstart, (4) itemid, (5) id, and (6) action parameters in index.php.	2006-05-01 2006-05-01	4.7	CVE-2006-2124 OTHER-REF FRSIRT SECUNIA

WilsonNCAreaBusinesses -- PHP Newsfeed	Multiple SQL injection vulnerabilities in PHP Newsfeed 20040723 allow remote attackers to execute arbitrary SQL commands via the (1) name parameter to (a) deltables.php, (2) select, (3) header, (4) url, (5) source, or (6) time parameters to (b) manualsubmit.php, (7) num parameter to (c) delete.php, or (8) tablename parameter to (d) searchnews.php.	2006-04-30 2006-05-02	4.7	CVE-2006-2139 OTHER-REF FRSIRT SECUNIA
X7 Group -- X7 Chat	Directory traversal vulnerability in help/index.php in X7 Chat 2.0 and earlier allows remote attackers to include arbitrary files via .. (dot dot) sequences in the help_file parameter.	unknown 2006-05-03	4.7	CVE-2006-2156 BUGTRAQ BID SECUNIA

Back to top

Low Vulnerabilities

Primary Vendor -- Product	Description	Discovered Published	CVSS Score	Source & Patch Info
	** REJECT ** DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: CVE-2005-3779. Reason: This candidate is a duplicate of CVE-2005-3779. Notes: All CVE users should reference CVE-2005-3779 instead of this candidate. All references and descriptions in this candidate have been removed to prevent accidental usage.	2005-11-11 2006-05-01	0.0	CVE-2006-2125
321soft -- PhP-Gallery	Absolute path traversal vulnerability in index.php in 321soft PhP-Gallery 0.9 allows remote attackers to browse arbitrary directories via the path parameter.	2006-05-03 2006-05-05	2.3	CVE-2006-2211 OTHER-REF BID FRSIRT SECUNIA
Advanced Poll -- Advanced Poll	include/class_poll.php in Advanced Poll 2.0.4 uses the HTTP_X_FORWARDED_FOR (X-Forwarded-For HTTP header) to identify the IP address of a client, which makes it easier for remote attackers to spoof the source IP and bypass voting restrictions.	unknown 2006-05-01	2.3	CVE-2006-2131 EVULN
Albinator -- Albinator	Multiple cross-site scripting (XSS) vulnerabilities in albinator 2.0.8 and earlier allow remote attackers to inject arbitrary web script or HTML via the (1) cid parameter to dlisting.php or (2) preloadSlideShow parameter to showpic.php.	2006-05-03 2006-05-04	2.3	CVE-2006-2181 OTHER-REF BID FRSIRT
Artmedic Webdesign -- Artmedic Event	PHP remote file inclusion vulnerability in event/index.php in Artmedic Event allows remote attackers to execute arbitrary code via a URL in the page parameter.	2006-05-01 2006-05-01	2.3	CVE-2006-2119 OTHER-REF BUGTRAQ OTHER-REF BID FRSIRT SECUNIA
Best Practical Solutions -- RT: Request Tracker	RT: Request Tracker 3.5.HEAD allows remote attackers to obtain sensitive information via the Rows parameter in Dist/Display.html, which reveals the installation path in an error message.	unknown 2006-05-04	2.3	CVE-2006-2169 OTHER-REF
BitDamaged -- geoBlog	Cross-site scripting (XSS) vulnerability in viewcat.php in geoBlog 1.0 allows remote attackers to inject arbitrary web script or HTML via the cat parameter.	2006-05-02 2006-05-04	2.3	CVE-2006-2177 BUGTRAQ OTHER-REF BID
Chadha Software Technologies -- phpkb Knowledge Base	Cross-site scripting (XSS) vulnerability in search.php in PHPKB Knowledge Base allows remote attackers to inject arbitrary web script or HTML via the searchkeyword parameter. NOTE: the original researcher claims that the vendor disputed the vulnerability, saying that only the vendor's own demo page was affected. As of 20060503, there is no public information regarding whether this dispute is valid or invalid.	unknown 2006-05-04	2.3	CVE-2006-2184 OTHER-REF FRSIRT SECUNIA
CMScout -- CMScout	Multiple cross-site scripting (XSS) vulnerabilities in CMScout 1.10 and earlier allow remote attackers to inject arbitrary web script or HTML via (1) the Body field of a private message (PM), (2) BBCode, or (3) a forum post.	2006-05-02 2006-05-04	3.3	CVE-2006-2188 BUGTRAQ BID
Collaborative Portal Server Project -- Collaborative Portal Server	Cross-site scripting (XSS) vulnerability in popup_image in Collaborative Portal Server (CPS) 3.4.0 and earlier allows remote attackers to inject arbitrary web script or HTML via the pos argument.	2006-04-30 2006-05-02	2.3	CVE-2006-2141 OTHER-REF SECUNIA
Computer Associates -- Resource Initialization Manager	Unspecified vulnerability in CA CAI Resource Initialization Manager (CAIRIM) 1.x before 20060502, as used in z/OS Common Services and the LMP component in multiple products, allows attackers to violate integrity via a certain "problem state program" that uses SVC to gain access to supervisor state, key 0.	unknown 2006-05-04	3.3	CVE-2006-2201 COMPUTER ASSOCIATES COMPUTER ASSOCIATES FRSIRT SECUNIA

DeltaScripts -- Pro Publish	Direct static code injection vulnerability in Pro Publish 2.0 allows rmeote authenticated adminitrators to execute arbitrary PHP code by editing certain settings, which are stored in set_inc.php.	2006-04-30 2006-05-01	2.8	CVE-2006-2129 OTHER-REF BID FRSIRT SECUNIA
Desert Dog Software -- Pinnacle Cart	Cross-site scripting (XSS) vulnerability in index.php in Pinnacle Cart 3.33 and earlier allows remote attackers to inject arbitrary web script or HTML via the setbackurl parameter.	unknown 2006-05-04	1.9	CVE-2006-2163 OTHER-REF BID FRSIRT SECUNIA
Devsyn -- Open Bulletin Board	Open Bulletin Board (OpenBB) 1.0.8 allows remote attackers to obtain the full path of the web server via an invalid pforums parameter to (1) misc.php and (2) member.php.	2006-04-28 2006-05-05	2.3	CVE-2006-2216 BUGTRAQ
DUclassified -- DUclassified	SQL injection vulnerability in detail.asp in DUclassified allows remote attackers to execute arbitrary SQL commands via the iPro parameter. NOTE: the provenance of this information is unknown; the details are obtained solely from third party information.	unknown 2006-05-01	3.3	CVE-2006-2132 SECURITY FOCUS BID
Extrosoft -- Thyme	Cross-site scripting (XSS) vulnerability in Thyme 1.3 allows remote attackers to inject arbitrary web script or HTML via the search page.	2006-04-29 2006-05-01	2.3	CVE-2006-2117 BUGTRAQ BID FRSIRT SECUNIA
EZB Systems -- UltraISO	Directory traversal vulnerability in UltraISO 8.0.0.1392 allows remote attackers to write arbitrary files via a .. (dot dot) in a filename in an ISO image.	2006-04-18 2006-04-29	2.3	CVE-2006-2099 BUGTRAQ OTHER-REF FRSIRT SECUNIA BID SECTRACK
Hostapd -- Hostapd	Hostapd 0.3.7-2 allows remote attackers to cause a denial of service (segmentation fault) via an unspecified value in the key_data_length field of an EAPoL frame.	2006-05-03 2006-05-05	2.3	CVE-2006-2213 OTHER-REF FRSIRT SECUNIA
I-Rater -- I-Rater Platinum	PHP remote file include vulnerability in admin/config_settings.tpl.php in I-RATER Platinum allows remote attackers to execute arbitrary code via a URL in the include_path parameter. NOTE: this is a different vector, and possibly a different vulnerability, than CVE-2006-1929.	2006-04-28 2006-05-01	2.3	CVE-2006-2121 BUGTRAQ BID
Invision Power Services -- Invision Power Board	SQL injection vulnerability in the topic deletion functionality (post_delete function in func_mod.php) for Invision Power Board 2.1.5 allows remote authenticated moderators to execute arbitrary SQL commands via the selectedpids parameter, which bypasses an integer value check when the $id variable is an array.	2006-04-28 2006-05-05	2.8	CVE-2006-2204 BUGTRAQ BUGTRAQ OTHER-REF BID FRSIRT SECUNIA
JBMC Software -- DirectAdmin	Cross-site scripting (XSS) vulnerability in HTM_PASSWD in DirectAdmin Hosting Management allows remote attackers to inject arbitrary web script or HTML via the domain parameter.	unknown 2006-05-03	2.3	CVE-2006-2153 BUGTRAQ FRSIRT SECUNIA
Jcink -- TextFileBB	Multiple cross-site scripting (XSS) vulnerabilities in TextFileBB 1.0.16 allow remote attackers to inject arbitrary web script or HTML via Javascript events such as "onmouseover" in the (1) color, (2) size, or (3) url bbcode tags.	2006-04-29 2006-05-02	2.3	CVE-2006-2143 BUGTRAQ BID SECUNIA
KMiNT21 Software -- Golden FTP Server	Buffer overflow in Golden FTP Server Pro 2.70 allows remote attackers to cause a denial of service (application crash) via a long argument to the (1) NLST or (2) APPE commands, as demonstrated by the Infigo FTPStress Fuzzer.	2005-11-12 2006-05-04	2.3	CVE-2006-2180 BUGTRAQ OTHER-REF BID FRSIRT SECUNIA
libTIFF -- libTIFF	The TIFFToRGB function in libtiff before 3.8.1 allows remote attackers to cause a denial of service (crash) via a crafted TIFF image with Yr/Yg/Yb values that exceed the YCR/YCG/YCB values, which triggers an out-of-bounds read.	2006-04-26 2006-05-01	1.6	CVE-2006-2120 OTHER-REF OTHER-REF MANDRIVA UBUNTU BID SECUNIA SECUNIA

Linux -- Linux kernel	The selinux_ptrace logic in hooks.c in SELinux for Linux 2.6.6 allows local users with ptrace permissions to change the tracer SID to an SID of another process.	2006-03-11 2006-05-05	1.6	CVE-2006-1052 MLIST MLIST OTHER-REF UBUNTU BID SECUNIA
Linux -- Linux kernel	The SCTP-netfilter code in Linux kernel before 2.6.16.13 allows remote attackers to trigger a denial of service (infinite loop) via unknown vectors that cause an invalid SCTP chunk size to be processed by the for_each_sctp_chunk function.	unknown 2006-05-03	2.3	CVE-2006-1527 OTHER-REF FRSIRT
MySQL -- MySQL	The check_connection function in sql_parse.cc in MySQL 4.0.x up to 4.0.26, 4.1.x up to 4.1.18, and 5.0.x up to 5.0.20 allows remote attackers to read portions of memory via a username without a trailing null byte, which causes a buffer over-read.	2006-05-02 2006-05-05	2.3	CVE-2006-1516 BUGTRAQ OTHER-REF OTHER-REF OTHER-REF FRSIRT SECTRACK SECUNIA
MySQL -- MySQL	sql_parse.cc in MySQL 4.0.x up to 4.0.26, 4.1.x up to 4.1.18, and 5.0.x up to 5.0.20 allows remote attackers to obtain sensitive information via a COM_TABLE_DUMP request with an incorrect packet length, which includes portions of memory in an error message.	2006-05-02 2006-05-05	2.3	CVE-2006-1517 BUGTRAQ OTHER-REF OTHER-REF OTHER-REF FRSIRT SECTRACK SECUNIA
MySQL -- MySQL	Buffer overflow in the open_table function in sql_base.cc in MySQL 4.0.x up to 4.0.26, 4.1.x up to 4.1.18, and 5.0.x up to 5.0.20 might allow remote attackers to execute arbitrary code via crafted COM_TABLE_DUMP packets with invalid length values.	2006-05-02 2006-05-05	2.3	CVE-2006-1518 BUGTRAQ OTHER-REF OTHER-REF OTHER-REF FRSIRT SECTRACK SECUNIA
Nagios -- Nagios	Buffer overflow in CGI scripts in Nagios 1.x before 1.4 and 2.x before 2.3 allows remote attackers to execute arbitrary code via a negative content length (Content-Length) HTTP header.	unknown 2006-05-03	2.3	CVE-2006-2162 OTHER-REF OTHER-REF
NeoMail -- NeoMail	Cross-site scripting (XSS) vulnerability in neomail.pl in NeoMail 1.29 allows remote attackers to inject arbitrary web script or HTML via the sessionid parameter.	2006-04-28 2006-05-02	2.3	CVE-2006-2138 BUGTRAQ BID SECUNIA
NetBSD -- NetBSD	The audio_write function in NetBSD 3.0 allows local users to cause a denial of service (kernel crash) by using the audiosetinfo ioctl to change the sample rate of an audio device.	2006-04-19 2006-05-05	1.6	CVE-2006-2205 NETBSD SECTRACK
Open WebMail -- Open WebMail	Cross-site scripting (XSS) vulnerability in ow-shared.pl in OpenWebMail (OWM) 2.51 and earlier allows remote attackers to inject arbitrary web script or HTML via the sessionid parameter in (1) openwebmail-send.pl, (2) openwebmail-advsearch.pl, (3) openwebmail-folder.pl, (4) openwebmail-prefs.pl, (5) openwebmail-abook.pl, (6) openwebmail-read.pl, (7) openwebmail-cal.pl, and (8) openwebmail-webdisk.pl. NOTE: the openwebmail-main.pl vector is already covered by CVE-2005-2863.	unknown 2006-05-04	3.3	CVE-2006-2190 BLOGSPOT MLIST OPENWEBMAIL OPENWEBMAIL SECUNIA XF
Pentasoft Corp. -- Avactis Shopping Cart	Multiple cross-site scripting (XSS) vulnerabilities in Avactis Shopping Cart 0.1.2 and earlier allow remote attackers to inject arbitrary web script or HTML via the (1) category_id parameter in (a) store_special_offers.php and (b) store.php and (2) prod_id parameter in (c) product_info.php. NOTE: this issue might be resultant from SQL injection.	unknown 2006-05-04	1.9	CVE-2006-2165 OTHER-REF
Planetluc -- MyNews	Multiple cross-site scripting (XSS) vulnerabilities in mynews.inc.php in MyNews 1.6.2 allow remote attackers to inject arbitrary web script or HTML via the (1) hash and (2) page parameters.	2006-05-03 2006-05-05	2.3	CVE-2006-2208 OTHER-REF BID FRSIRT SECUNIA XF
Plogger -- Plogger	SQL injection vulnerability in gallery.php in Plogger Beta 2.1 and earlier allows remote attackers to execute arbitrary SQL commands via the id parameter, when the level is set to "slideshow". NOTE: This is a different vulnerability than CVE-2005-4246.	unknown 2006-05-03	2.3	CVE-2006-2157 OTHER-REF

resmgr -- resmgrd	resmgrd in resmgr for SUSE Linux and other distributions does not properly handle when access to a USB device is granted by using "usb:," notation, which grants access to all USB devices and allows local users to bypass intended restrictions. NOTE: this is a different vulnerability than CVE-2005-4788.	2006-04-30 2006-05-02	3.3	CVE-2006-2147 SUSE DEBIAN
Russcom Network -- Loginphp	CRLF injection vulnerability in help.php in Russcom Network Loginphp allows remote attackers to spoof e-mails and inject MIME headers via CRLF sequences in the email address.	2006-05-02 2006-05-03	2.3	CVE-2006-2159 BUGTRAQ BID OSVDB SECUNIA
Russcom Network -- Loginphp	Cross-site scripting (XSS) vulnerability in Russcom Network Loginphp (Russcom.Loginphp) allows remote attackers to inject arbitrary web script or HTML via the username field when registering.	2006-05-02 2006-05-03	2.3	CVE-2006-2160 BUGTRAQ BID OSVDB SECUNIA
SloughFlash -- SF-Users	Cross-site scripting (XSS) vulnerability in SloughFlash SF-Users 1.0, possibly in register.php, allows remote attackers to inject arbitrary web script or HTML by setting the username field to contain JavaScript in the SRC attribute of an IMG element.	unknown 2006-05-04	2.3	CVE-2006-2167 BUGTRAQ BID FRSIRT SECUNIA
Virtual Hosting Control System -- Virtual Hosting Control System	Multiple cross-site scripting (XSS) vulnerabilities in admin/server_day_stats.php in Virtual Hosting Control System (VHCS) allow remote attackers to inject arbitrary web script or HTML via the (1) day, (2) month, or (3) year parameter.	2006-05-02 2006-05-04	2.3	CVE-2006-2174 BUGTRAQ BID SECUNIA
X.org -- X11R6	Buffer overflow in the X render (Xrender) extension in X.org X server 6.8.0 up to allows attackers to cause a denial of service (crash), as demonstrated by the (1) XRenderCompositeTriStrip and (2) XRenderCompositeTriFan requests in the rendertest from XCB xcb/xcb-demo, which leads to an incorrect memory allocation due to a typo in an expression that uses a "&" instead of a "*" operator. NOTE: the subject line of the original announcement used an incorrect CVE number for this issue.	2006-05-02 2006-05-02	1.6	CVE-2006-1526 MLIST OTHER-REF GENTOO MANDRIVA OPENBSD REDHAT SUSE UBUNTU FRSIRT SECTRACK SECUNIA SECUNIA SECUNIA SECUNIA SECUNIA SECUNIA SECUNIA
Zenphoto -- zenphoto	zenphoto 1.0.1 beta and earlier allow remote attackers to obtain sensitive information via a direct request for the (1) /photos/themes/default/ and (2) /photos/themes/testing/ URIs, which reveals the path in an error message.	unknown 2006-05-04	2.3	CVE-2006-2186 BUGTRAQ OTHER-REF BID

Back to top

Last updated May 08, 2006

=